Article

Chinese Science Bulletin

Quantum Information

January 2011 Vol.56 No.1: 24–28
doi: 10.1007/s11434-010-4208-y

Quantum key distribution using four-level particles

YAN Tao[1,2] & YAN FengLi[1,2*]

[1] *College of Physics Science and Information Engineering, Hebei Normal University, Shijiazhuang 050016, China;*
[2] *Hebei Advanced Thin Films Laboratory, Shijiazhuang 050016, China*

Received May 29, 2010; accepted August 13, 2010

We present a quantum key distribution protocol based on four-level particle entanglement. Furthermore, a controlled quantum key distribution protocol is proposed using three four-level particles. We show that the two protocols are secure.

quantum key distribution, four-level particles, entanglement

Citation: Yan T, Yan F L. Quantum key distribution using four-level particles. Chinese Sci Bull, 2011, 56: 24–28, doi: 10.1007/s11434-010-4208-y

Quantum key distribution (QKD) is one of the most important branches of quantum cryptography, and plays an important role in perfectly secure communication between two parties. In classic cryptography, there is nothing to prevent an eavesdropper from monitoring the key distribution channel without being detected by legitimate users. In quantum cryptography, the principle of quantum mechanics was introduced to ensure the security of the key distribution channel. Since the seminal work of Bennett and Brassard [1], quantum cryptography has developed quickly [2–19]. Using Einstein-Podolsky-Rosen (EPR) [20] correlations, Ekert [3] suggested a QKD protocol, in which one can certify that the particles of EPR pairs are safely transmitted in the quantum channel using Bell's theorem [21]. In 1992, Bennett et al. [4] proposed a simpler EPR protocol without invoking Bell's theorem. Long et al. [6] put forward a QKD protocol using the block transmission method to ensure the security of the key distribution channel.

In this paper, we suggest a QKD protocol based on four-level particle entanglement. Then a controlled quantum key distribution protocol is proposed using three entangled four-level particles as the quantum key distribution channel. The security of the key distribution channels is guaranteed using the block transmission method proposed by Long et al. [6].

*Corresponding author (email: flyan@hebtu.edu.cn)

1 A quantum key distribution protocol using two entangled four-level particles as the quantum channel

Suppose that two legitimate correspondents, Alice and Bob, share a number of the following entangled quantum states:

$$\begin{aligned}|\chi\rangle_{AB} &= \frac{1}{2}(|01\rangle+|10\rangle-|23\rangle-|32\rangle)_{AB}\\ &= \frac{1}{2}(|\psi^-\rangle|\phi^+\rangle+|\phi^-\rangle|\psi^+\rangle\\ &\quad +|\psi^+\rangle|\phi^-\rangle+|\phi^+\rangle|\psi^-\rangle),\end{aligned} \tag{1}$$

which is also called the quantum channel. Here the four-level particles A and B belong to Alice and Bob, respectively; the states $|i\rangle$ (i=0, 1, 2, 3) stand for the four eigenstates of the four-level particles A and B; the states $|\phi^{\pm}\rangle$, $|\psi^{\pm}\rangle$ are well defined as

$$\begin{aligned}&|\phi^+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|3\rangle),\ |\phi^-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|3\rangle),\\ &|\psi^+\rangle=\frac{1}{\sqrt{2}}(|1\rangle+|2\rangle),\ |\psi^-\rangle=\frac{1}{\sqrt{2}}(|1\rangle-|2\rangle).\end{aligned} \tag{2}$$

Obviously, the states in eq. (2) are orthogonal to each other and constitute a basis of four-dimensional Hilbert space.

Obtaining a number of state $|\chi\rangle_{AB}$ could have come about in many different ways. For example, Alice could prepare the pairs and then send half of each to Bob, or vice versa. Alternatively, a third party could prepare the pairs and send the halves to Alice and Bob. Or, they could have met some time ago and shared them, storing them until the present.

We introduce the following operators:

$$\begin{aligned}\sigma_x &= |3\rangle\langle 0| + |0\rangle\langle 3| + |1\rangle\langle 2| + |2\rangle\langle 1|,\\ v_x &= |2\rangle\langle 0| + |0\rangle\langle 2| + |3\rangle\langle 1| + |1\rangle\langle 3|,\\ \sigma_z &= |3\rangle\langle 3| + |1\rangle\langle 1| - |0\rangle\langle 0| - |2\rangle\langle 2|,\\ v_z &= |2\rangle\langle 2| + |3\rangle\langle 3| - |0\rangle\langle 0| - |1\rangle\langle 1|.\end{aligned} \tag{3}$$

Clearly, σ_x, v_x, σ_z, v_z are Hermitian operators and

$$\sigma_x^2 = v_x^2 = \sigma_z^2 = v_z^2 = I. \tag{4}$$

Here I is an identity operator in four-dimensional Hilbert space. Thus the eigenvalues of the operators σ_x, v_x, σ_z, v_z can only be 1 or –1.

It is easy to prove that

$$\sigma_x^A \otimes \sigma_x^B |\chi\rangle_{AB} = -|\chi\rangle_{AB}, \tag{5.1}$$

$$v_x^A \otimes v_x^B |\chi\rangle_{AB} = -|\chi\rangle_{AB}, \tag{5.2}$$

$$\sigma_z^A \otimes \sigma_z^B |\chi\rangle_{AB} = -|\chi\rangle_{AB}, \tag{5.3}$$

$$v_z^A \otimes v_z^B |\chi\rangle_{AB} = |\chi\rangle_{AB}. \tag{5.4}$$

Next we will show that if a quantum state $|\Psi\rangle_{ABE}$ satisfies

$$\sigma_x^A \otimes \sigma_x^B |\Psi\rangle_{ABE} = -|\Psi\rangle_{ABE}, \tag{6.1}$$

$$v_x^A \otimes v_x^B |\Psi\rangle_{ABE} = -|\Psi\rangle_{ABE}, \tag{6.2}$$

$$\sigma_z^A \otimes \sigma_z^B |\Psi\rangle_{ABE} = -|\Psi\rangle_{ABE}, \tag{6.3}$$

$$v_z^A \otimes v_z^B |\Psi\rangle_{ABE} = |\Psi\rangle_{ABE}, \tag{6.4}$$

then the quantum state $|\Psi\rangle_{ABE} = |\chi\rangle_{AB}|\alpha\rangle_E$. Here E denotes the environment of the system consisting of particles A and B; $|\alpha\rangle_E$ is the quantum state of the environment. Of course, the eavesdropper is included in the environment.

Apparently, the most general state $|\Psi\rangle_{ABE}$ is of the form

$$\begin{aligned}|\Psi\rangle_{ABE} =& |00\rangle_{AB}|\alpha_1\rangle_E + |01\rangle_{AB}|\alpha_2\rangle_E + |02\rangle_{AB}|\alpha_3\rangle_E\\ &+ |03\rangle_{AB}|\alpha_4\rangle_E + |10\rangle_{AB}|\alpha_5\rangle_E + |11\rangle_{AB}|\alpha_6\rangle_E\\ &+ |12\rangle_{AB}|\alpha_7\rangle_E + |13\rangle_{AB}|\alpha_8\rangle_E + |20\rangle_{AB}|\alpha_9\rangle_E\\ &+ |21\rangle_{AB}|\alpha_{10}\rangle_E + |22\rangle_{AB}|\alpha_{11}\rangle_E + |23\rangle_{AB}|\alpha_{12}\rangle_E\\ &+ |30\rangle_{AB}|\alpha_{13}\rangle_E + |31\rangle_{AB}|\alpha_{14}\rangle_E + |32\rangle_{AB}|\alpha_{15}\rangle_E\\ &+ |33\rangle_{AB}|\alpha_{16}\rangle_E,\end{aligned} \tag{7}$$

where $|\alpha_i\rangle_E$, i=1, 2,…16, stand for the un-normalized quantum states of the environment.

By considering eq. (6.1) we obtain

$$\begin{aligned}&|\alpha_1\rangle_E = -|\alpha_{16}\rangle_E,\ |\alpha_2\rangle_E = -|\alpha_{15}\rangle_E,\\ &|\alpha_3\rangle_E = -|\alpha_{14}\rangle_E,\ |\alpha_4\rangle_E = -|\alpha_{13}\rangle_E,\\ &|\alpha_5\rangle_E = -|\alpha_{12}\rangle_E,\ |\alpha_6\rangle_E = -|\alpha_{11}\rangle_E,\\ &|\alpha_7\rangle_E = -|\alpha_{10}\rangle_E,\ |\alpha_8\rangle_E = -|\alpha_9\rangle_E.\end{aligned} \tag{8}$$

Thus eq. (7) becomes

$$\begin{aligned}|\Psi\rangle_{ABE} =& (|00\rangle - |33\rangle)_{AB}|\alpha_1\rangle_E + (|01\rangle - |32\rangle)_{AB}|\alpha_2\rangle_E\\ &+ (|02\rangle - |31\rangle)_{AB}|\alpha_3\rangle_E + (|03\rangle - |30\rangle)_{AB}|\alpha_4\rangle_E\\ &+ (|10\rangle - |23\rangle)_{AB}|\alpha_5\rangle_E + (|11\rangle - |22\rangle)_{AB}|\alpha_6\rangle_E\\ &+ (|12\rangle - |21\rangle)_{AB}|\alpha_7\rangle_E + (|13\rangle - |20\rangle)_{AB}|\alpha_8\rangle_E.\end{aligned} \tag{9}$$

Substituting eq. (9) into eq. (6.2), we have

$$\begin{aligned}&|\alpha_1\rangle_E = |\alpha_6\rangle_E,\ |\alpha_2\rangle_E = |\alpha_5\rangle_E,\\ &|\alpha_3\rangle_E = |\alpha_8\rangle_E,\ |\alpha_4\rangle_E = |\alpha_7\rangle_E.\end{aligned} \tag{10}$$

Hence, the quantum state $|\Psi\rangle_{ABE}$ can be written as

$$\begin{aligned}|\Psi\rangle_{ABE} =& (|00\rangle - |33\rangle + |11\rangle - |22\rangle)_{AB}|\alpha_1\rangle_E\\ &+ (|01\rangle - |32\rangle + |10\rangle - |23\rangle)_{AB}|\alpha_2\rangle_E\\ &+ (|02\rangle - |31\rangle + |13\rangle - |20\rangle)_{AB}|\alpha_3\rangle_E\\ &+ (|03\rangle - |30\rangle + |12\rangle - |21\rangle)_{AB}|\alpha_4\rangle_E.\end{aligned} \tag{11}$$

Using eq. (6.3) we can obtain

$$|\alpha_1\rangle_E = 0, |\alpha_3\rangle_E = 0. \tag{12}$$

This leads to

$$\begin{aligned}|\Psi\rangle_{ABE} =& (|01\rangle - |32\rangle + |10\rangle - |23\rangle)_{AB}|\alpha_2\rangle_E\\ &+ (|03\rangle - |30\rangle + |12\rangle - |21\rangle)_{AB}|\alpha_4\rangle_E.\end{aligned} \tag{13}$$

Since the quantum state $|\Psi\rangle_{ABE}$ should satisfy eq. (6.4), there must be

$$|\alpha_4\rangle_E = 0. \tag{14}$$

Thus we arrive at the conclusion, which is

$$|\Psi\rangle_{ABE} = (|01\rangle - |32\rangle + |10\rangle - |23\rangle)_{AB}|\alpha_2\rangle_E. \tag{15}$$

As a matter of fact, $|\Psi\rangle_{ABE}$ is just the quantum state $|\chi\rangle_{AB}|\alpha\rangle_E$. This means the proof has been completed.

The above result indicates that when the quantum state satisfies eq. (6), it must be $|\chi\rangle_{AB}|\alpha\rangle_E$. This means that the quantum channel shared by Alice and Bob is entirely uncorrelated with the eavesdropper. Thus it is impossible for the eavesdropper to obtain the secret key.

Therefore, the legitimate correspondents, Alice and Bob can check whether the quantum channel is $|\chi\rangle_{AB}$. Each of them randomly chooses the operators σ_x, v_x, σ_z, v_z to measure

the entangled states they shared. After a series of the entangled states have been measured, Alice and Bob announce the operators and the measurement outcomes. If eq. (6) is satisfied by all measurement outcomes, then the quantum channel is the entangled quantum state $|\chi\rangle_{AB}$. This means that the quantum channel shared by Alice and Bob is secure. If an eavesdropper wants to obtain the secret key between Alice and Bob, he/she must entangle his/her qubits with the particles *A* and *B*. In this case, the measurement outcomes of Alice and Bob cannot satisfy eq. (6) exactly. Thus the eavesdropper will be found easily, and Alice and Bob will restart the protocol.

It should be noted that Alice and Bob need to authenticate each other before the protocol and trust authenticated classical messages are received from each other in the protocol. Therefore, the eavesdropper cannot behave as Alice or Bob in the eavesdropping procedure.

If the quantum channel is secure, then the two correspondents, Alice and Bob could use it to distribute quantum keys by the following steps:

(i) Alice and Bob measure their respective particles *A*, *B* on the same basis as defined in eq. (2).

(ii) The quantum channel $|\chi\rangle_{AB}$ shared by Alice and Bob would read

$$|\chi\rangle_{AB}=\frac{1}{2}(|\psi^-\rangle|\varphi^+\rangle+|\varphi^-\rangle|\psi^+\rangle+|\psi^+\rangle|\varphi^-\rangle+|\varphi^+\rangle|\psi^-\rangle)_{AB}. \tag{16}$$

In eq. (16), the four states $\{|\phi^+\rangle,|\phi^-\rangle,|\psi^+\rangle,|\psi^-\rangle\}$ would be coded into two bits of classical information as they are orthogonal to each other. One bit would be used to discriminate the states $|\phi\rangle$ or $|\psi\rangle$ which we call a parity bit, and the other bit would be used to discriminate the superscripts of the states $|\phi^{\pm}\rangle$ or $|\psi^{\pm}\rangle$ which we call a phase bit.

(iii) From a series of measurement results, they randomly choose some to reexamine the security of the quantum channel. If their results are well correlated, then the quantum channel can be considered secure. Otherwise, they should restart the protocol.

(iv) If the quantum channel is secure by the above examination, we could use the parity bit and the phase bit of the measurement results as the secret key.

So far, a secret key has been set up between the two correspondents using the entangled four-level particles. The security of the protocol is based on the laws of physics.

2 A controlled quantum key distribution protocol using three four-level particles

Assume that the controller Alice, and the two correspondents, Bob and Charlie, share a quantum channel consisting of a number of the three entangled four-level particles

$$\begin{aligned}|\chi\rangle_{ABC}=&\frac{1}{2\sqrt{2}}(|000\rangle+|011\rangle+|101\rangle+|110\rangle\\&+|223\rangle+|232\rangle+|322\rangle+|333\rangle)_{ABC}\\=&\frac{1}{4}[|\phi^+\rangle_A(|\phi^+\rangle|\phi^+\rangle+|\phi^-\rangle|\phi^-\rangle\\&+|\psi^+\rangle|\psi^+\rangle+|\psi^-\rangle|\psi^-\rangle)_{BC}\\&+|\phi^-\rangle_A(|\phi^-\rangle|\phi^+\rangle+|\phi^+\rangle|\phi^-\rangle\\&+|\psi^+\rangle|\psi^-\rangle+|\psi^-\rangle|\psi^+\rangle)_{BC}\\&+|\psi^+\rangle_A(|\psi^+\rangle|\phi^+\rangle+|\phi^+\rangle|\psi^+\rangle\\&+|\psi^-\rangle|\phi^-\rangle+|\phi^-\rangle|\psi^-\rangle)_{BC}\\&+|\psi^-\rangle_A(|\psi^-\rangle|\phi^+\rangle+|\phi^-\rangle|\psi^+\rangle\\&+|\psi^+\rangle|\phi^-\rangle+|\phi^+\rangle|\psi^-\rangle)_{BC}].\end{aligned} \tag{17}$$

Here the four-level particles *A*, *B* and *C* belong to Alice, Bob and Charlie, respectively.

Now we introduce another two measurement operators:

$$\begin{aligned}\varepsilon_x=&|2\rangle\langle3|+|3\rangle\langle2|+|0\rangle\langle1|+|1\rangle\langle0|,\\o_z=&|3\rangle\langle3|-|1\rangle\langle1|+|0\rangle\langle0|+|2\rangle\langle2|.\end{aligned} \tag{18}$$

It is easy to prove that ε_x, o_z are Hermitian operators and

$$\varepsilon_x^2=o_z^2=I. \tag{19}$$

Therefore, the eigenvalues of the operators ε_x, o_z are 1 or −1.

One can check that $|\chi\rangle_{ABC}$ satisfies

$$\begin{aligned}&\sigma_x^A\otimes\sigma_x^B\otimes\sigma_x^C|\chi\rangle_{ABC}=|\chi\rangle_{ABC},\\&o_z^A\otimes o_z^B\otimes o_z^C|\chi\rangle_{ABC}=|\chi\rangle_{ABC},\\&\varepsilon_x^A\otimes\varepsilon_x^B\otimes I^C|\chi\rangle_{ABC}=|\chi\rangle_{ABC},\\&I^A\otimes\varepsilon_x^B\otimes\varepsilon_x^C|\chi\rangle_{ABC}=|\chi\rangle_{ABC}.\end{aligned} \tag{20}$$

Next, we will prove that if $|\psi\rangle_{ABCE}$ satisfies the following equation:

$$\sigma_x^A\otimes\sigma_x^B\otimes\sigma_x^C|\psi\rangle_{ABCE}=|\psi\rangle_{ABCE}, \tag{21.1}$$

$$o_z^A\otimes o_z^B\otimes o_z^C|\psi\rangle_{ABCE}=|\psi\rangle_{ABCE}, \tag{21.2}$$

$$\varepsilon_x^A\otimes\varepsilon_x^B\otimes I^C|\psi\rangle_{ABCE}=|\psi\rangle_{ABCE}, \tag{21.3}$$

$$I^A\otimes\varepsilon_x^B\otimes\varepsilon_x^C|\psi\rangle_{ABCE}=|\psi\rangle_{ABCE}, \tag{21.4}$$

then $|\psi\rangle_{ABCE}=|\chi\rangle_{ABC}|\beta\rangle_E$ holds. Here *E* still stands for the environment.

The general formation of the quantum state of the three four-level particles and the environment should be

$$
\begin{aligned}
|\psi\rangle_{ABCE} =& |000\rangle|\beta_{000}\rangle+|001\rangle|\beta_{001}\rangle+|002\rangle|\beta_{002}\rangle\\
&+|003\rangle|\beta_{003}\rangle+|010\rangle|\beta_{010}\rangle+|011\rangle|\beta_{011}\rangle\\
&+|012\rangle|\beta_{012}\rangle+|013\rangle|\beta_{013}\rangle+|020\rangle|\beta_{020}\rangle\\
&+|021\rangle|\beta_{021}\rangle+|022\rangle|\beta_{022}\rangle+|023\rangle|\beta_{023}\rangle\\
&+|030\rangle|\beta_{030}\rangle+|031\rangle|\beta_{031}\rangle+|032\rangle|\beta_{032}\rangle\\
&+|033\rangle|\beta_{033}\rangle+|100\rangle|\beta_{100}\rangle+|101\rangle|\beta_{101}\rangle\\
&+|102\rangle|\beta_{102}\rangle+|103\rangle|\beta_{103}\rangle+|110\rangle|\beta_{110}\rangle\\
&+|111\rangle|\beta_{111}\rangle+|112\rangle|\beta_{112}\rangle+|113\rangle|\beta_{113}\rangle\\
&+|120\rangle|\beta_{120}\rangle+|121\rangle|\beta_{121}\rangle+|122\rangle|\beta_{122}\rangle\\
&+|123\rangle|\beta_{123}\rangle+|130\rangle|\beta_{130}\rangle+|131\rangle|\beta_{131}\rangle\\
&+|132\rangle|\beta_{132}\rangle+|133\rangle|\beta_{133}\rangle+|200\rangle|\beta_{200}\rangle\\
&+|201\rangle|\beta_{201}\rangle+|202\rangle|\beta_{202}\rangle+|203\rangle|\beta_{203}\rangle\\
&+|210\rangle|\beta_{210}\rangle+|211\rangle|\beta_{211}\rangle+|212\rangle|\beta_{212}\rangle\\
&+|213\rangle|\beta_{213}\rangle+|220\rangle|\beta_{220}\rangle+|221\rangle|\beta_{221}\rangle\\
&+|222\rangle|\beta_{222}\rangle+|223\rangle|\beta_{223}\rangle+|230\rangle|\beta_{230}\rangle\\
&+|231\rangle|\beta_{231}\rangle+|232\rangle|\beta_{232}\rangle+|233\rangle|\beta_{233}\rangle\\
&+|300\rangle|\beta_{300}\rangle+|301\rangle|\beta_{301}\rangle+|302\rangle|\beta_{302}\rangle\\
&+|303\rangle|\beta_{303}\rangle+|310\rangle|\beta_{310}\rangle+|311\rangle|\beta_{311}\rangle\\
&+|312\rangle|\beta_{312}\rangle+|313\rangle|\beta_{313}\rangle+|320\rangle|\beta_{320}\rangle\\
&+|321\rangle|\beta_{321}\rangle+|322\rangle|\beta_{322}\rangle+|323\rangle|\beta_{323}\rangle\\
&+|330\rangle|\beta_{330}\rangle+|331\rangle|\beta_{331}\rangle+|332\rangle|\beta_{332}\rangle\\
&+|333\rangle|\beta_{333}\rangle. \qquad (22)
\end{aligned}
$$

Here $|\beta_i\rangle$, i=000, 001,…,333, are the states of the environment; $|klm\rangle$, k, l, m =0, 1, 2, 3, denote the states of the three four-level particles A, B, C.

According to eq. (21.1), we have

$$
\begin{aligned}
&|\beta_{000}\rangle=|\beta_{333}\rangle,\ |\beta_{001}\rangle=|\beta_{332}\rangle,\ |\beta_{002}\rangle=|\beta_{331}\rangle,\\
&|\beta_{003}\rangle=|\beta_{330}\rangle,\ |\beta_{010}\rangle=|\beta_{323}\rangle,\ |\beta_{011}\rangle=|\beta_{322}\rangle,\\
&|\beta_{012}\rangle=|\beta_{321}\rangle,\ |\beta_{013}\rangle=|\beta_{320}\rangle,\ |\beta_{020}\rangle=|\beta_{313}\rangle,\\
&|\beta_{021}\rangle=|\beta_{312}\rangle,\ |\beta_{022}\rangle=|\beta_{311}\rangle,\ |\beta_{023}\rangle=|\beta_{310}\rangle,\\
&|\beta_{030}\rangle=|\beta_{303}\rangle,\ |\beta_{031}\rangle=|\beta_{302}\rangle,\ |\beta_{032}\rangle=|\beta_{301}\rangle,\\
&|\beta_{033}\rangle=|\beta_{300}\rangle,\ |\beta_{100}\rangle=|\beta_{233}\rangle,\ |\beta_{101}\rangle=|\beta_{232}\rangle,\\
&|\beta_{102}\rangle=|\beta_{231}\rangle,\ |\beta_{103}\rangle=|\beta_{230}\rangle,\ |\beta_{110}\rangle=|\beta_{223}\rangle,\\
&|\beta_{111}\rangle=|\beta_{222}\rangle,\ |\beta_{112}\rangle=|\beta_{221}\rangle,\ |\beta_{113}\rangle=|\beta_{220}\rangle,\\
&|\beta_{120}\rangle=|\beta_{213}\rangle,\ |\beta_{121}\rangle=|\beta_{212}\rangle,\ |\beta_{122}\rangle=|\beta_{211}\rangle,\\
&|\beta_{123}\rangle=|\beta_{210}\rangle,\ |\beta_{130}\rangle=|\beta_{203}\rangle,\ |\beta_{131}\rangle=|\beta_{202}\rangle,\\
&|\beta_{132}\rangle=|\beta_{201}\rangle,\ |\beta_{133}\rangle=|\beta_{200}\rangle. \qquad (23)
\end{aligned}
$$

Thus we then obtain

$$
\begin{aligned}
|\psi\rangle_{ABCE} =& (|000\rangle+|333\rangle)|\beta_{000}\rangle+(|001\rangle+|332\rangle)|\beta_{001}\rangle\\
&+(|002\rangle+|331\rangle)|\beta_{002}\rangle+(|003\rangle+|330\rangle)|\beta_{003}\rangle\\
&+(|010\rangle+|323\rangle)|\beta_{010}\rangle+(|011\rangle+|322\rangle)|\beta_{011}\rangle\\
&+(|012\rangle+|321\rangle)|\beta_{012}\rangle+(|013\rangle+|320\rangle)|\beta_{013}\rangle\\
&+(|020\rangle+|313\rangle)|\beta_{020}\rangle+(|021\rangle+|312\rangle)|\beta_{021}\rangle\\
&+(|022\rangle+|311\rangle)|\beta_{022}\rangle+(|023\rangle+|310\rangle)|\beta_{023}\rangle\\
&+(|030\rangle+|303\rangle)|\beta_{030}\rangle+(|031\rangle+|302\rangle)|\beta_{031}\rangle\\
&+(|032\rangle+|301\rangle)|\beta_{032}\rangle+(|033\rangle+|300\rangle)|\beta_{033}\rangle\\
&+(|100\rangle+|233\rangle)|\beta_{100}\rangle+(|101\rangle+|232\rangle)|\beta_{101}\rangle\\
&+(|102\rangle+|231\rangle)|\beta_{102}\rangle+(|103\rangle+|230\rangle)|\beta_{103}\rangle\\
&+(|110\rangle+|223\rangle)|\beta_{110}\rangle+(|111\rangle+|222\rangle)|\beta_{111}\rangle\\
&+(|112\rangle+|221\rangle)|\beta_{112}\rangle+(|113\rangle+|220\rangle)|\beta_{113}\rangle\\
&+(|120\rangle+|213\rangle)|\beta_{120}\rangle+(|121\rangle+|212\rangle)|\beta_{121}\rangle\\
&+(|122\rangle+|211\rangle)|\beta_{122}\rangle+(|123\rangle+|210\rangle)|\beta_{123}\rangle\\
&+(|130\rangle+|203\rangle)|\beta_{130}\rangle+(|131\rangle+|202\rangle)|\beta_{131}\rangle\\
&+(|132\rangle+|201\rangle)|\beta_{132}\rangle+(|133\rangle+|200\rangle)|\beta_{133}\rangle. \qquad (24)
\end{aligned}
$$

Substituting it into eq. (21.2), we obtain

$$
\begin{aligned}
|\beta_{001}\rangle =& |\beta_{002}\rangle=|\beta_{010}\rangle=|\beta_{012}\rangle\\
=& |\beta_{013}\rangle=|\beta_{020}\rangle=|\beta_{021}\rangle\\
=& |\beta_{023}\rangle=|\beta_{031}\rangle=|\beta_{032}\rangle\\
=& |\beta_{100}\rangle=|\beta_{102}\rangle=|\beta_{103}\rangle\\
=& |\beta_{111}\rangle=|\beta_{112}\rangle=|\beta_{120}\rangle\\
=& |\beta_{121}\rangle=|\beta_{122}\rangle=|\beta_{123}\rangle\\
=& |\beta_{130}\rangle=|\beta_{132}\rangle=|\beta_{133}\rangle=0. \qquad (25)
\end{aligned}
$$

And it leads to

$$
\begin{aligned}
|\psi\rangle_{ABCE} =& (|000\rangle+|333\rangle)|\beta_{000}\rangle+(|003\rangle+|330\rangle)|\beta_{003}\rangle\\
&+(|011\rangle+|322\rangle)|\beta_{011}\rangle+(|022\rangle+|311\rangle)|\beta_{022}\rangle\\
&+(|030\rangle+|303\rangle)|\beta_{030}\rangle+(|033\rangle+|300\rangle)|\beta_{033}\rangle\\
&+(|101\rangle+|232\rangle)|\beta_{101}\rangle+(|110\rangle+|223\rangle)|\beta_{110}\rangle\\
&+(|113\rangle+|220\rangle)|\beta_{113}\rangle+(|131\rangle+|202\rangle)|\beta_{131}\rangle. \qquad (26)
\end{aligned}
$$

By the restriction of eq. (21.3), we obtain

$$
\begin{aligned}
&|\beta_{000}\rangle=|\beta_{110}\rangle,|\beta_{003}\rangle=|\beta_{113}\rangle,|\beta_{011}\rangle=|\beta_{101}\rangle,\\
&|\beta_{022}\rangle=|\beta_{030}\rangle=|\beta_{033}\rangle=|\beta_{131}\rangle=0. \qquad (27)
\end{aligned}
$$

This means

$$
\begin{aligned}
|\psi\rangle_{ABCE} =& (|110\rangle+|223\rangle+|000\rangle+|333\rangle)|\beta_{000}\rangle\\
&+(|113\rangle+|220\rangle+|003\rangle+|330\rangle)|\beta_{003}\rangle\\
&+(|101\rangle+|232\rangle+|011\rangle+|322\rangle)|\beta_{011}\rangle. \qquad (28)
\end{aligned}
$$

Eq. (21.4) further restricts $|\psi\rangle_{ABCE}$ to be of the form

$$
\begin{aligned}
|\psi\rangle_{ABCE} =& (|110\rangle+|223\rangle+|000\rangle+|333\rangle\\
&+|101\rangle+|232\rangle+|011\rangle+|322\rangle)|\beta_{000}\rangle\\
=& |\chi\rangle_{ABC}|\beta\rangle_E. \qquad (29)
\end{aligned}
$$

Thus the proof has been completed.

Based on the conclusion above, Alice, Bob and Charlie can check whether the quantum channel is $|\chi\rangle_{ABC}$. Each of them randomly selects the operators σ_x, ε_x, o_z and I to

measure the entangled states they share. After many of the entangled states have been measured, Alice, Bob and Charlie publish the operators and the measurement outcomes. If eq. (21) is satisfied by all the measurement outcomes, then the quantum channel is the entangled quantum state $|\chi\rangle_{ABC}$, meaning that the quantum channel shared by Alice, Bob and Charlie is entirely uncorrelated with the eavesdropper. If an eavesdropper is stealing the secret key between Alice and Bob, he/she must entangle his/her qubits with the particles A, B and C. Hence the quantum state of the particles A, B, C and E is not $|\chi\rangle_{ABC}|\beta\rangle_E$. In this case, the measurement outcomes of Alice, Bob and Charlie can not satisfy eq. (21) exactly, so the eavesdropper will easily be found. The legitimate users Alice, Bob and Charlie will restart the protocol. We assume that in the process of testing the security of the quantum channel, Alice, Bob and Charlie announce the true results.

If the quantum channel is secure, then the two correspondents, Bob and Charlie, can use it to distribute quantum keys controlled by Alice. The details are as follows:

(i) Alice, Bob and Charlie measure the rest of their respective particles A, B and C on the same basis as defined in eq. (2) and record the measurement results.

(ii) Evidently, the measurement results are correlated according to eq. (17). Hence, the measurement result is a secret key shared by Alice, Bob and Charlie. If the controller Alice permits Bob and Charlie to create a secret key, she should tell Bob and Charlie her measurement outcomes. With the message of Alice's measurement outcomes and Bob's measurement results, Bob can deduce Charlie's measurement results. At the same time, with the message of Alice's measurement outcomes and Charlie's measurement results, Charlie can obtain Bob's measurement results. Thus with Alice's permission Bob and Charlie can create a secret key based on the measurement results. However, if Alice does not announce her measurement outcomes, there is no way for Bob and Charlie to create a secret key using the quantum channel $|\chi\rangle_{ABC}$. This is just a controlled quantum key distribution. In other words, the quantum key distribution between Bob and Charlie is controlled by Alice. In fact, this controlled quantum key distribution protocol is just a secret sharing protocol [22–25].

3 Conclusion

We presented a quantum key distribution protocol based on four-level particle entanglement and described a controlled quantum key distribution protocol using three four-level particles. The security of the two protocols is guaranteed by the law of quantum physics.

This work was supported by the National Natural Science Foundation of China (10971247) and Hebei Provincial Natural Science Foundation (F2009000311, A2010000344).

1 Bennett C H, Brassard G. Quantum cryptography: Public-key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, System and Signal Processing. New York: IEEE, 1984. 175–179
2 Bennett C H. Quantum cryptography using any two non-orthogonal states. Phys Rev Lett, 1992, 68: 3121–3124
3 Ekert A. Quantum cryptography based on Bells theorem. Phys Rev Lett, 1991, 67: 661–664
4 Bennett C H, Brassard G, Mermin N D. Quantum cryptography without Bells theorem. Phys Rev Lett, 1992, 68: 557–559
5 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. Rev Mod Phys, 2002, 74: 145–195
6 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002, 65: 032302
7 Deng F G, Long G L. Controlled order rearrangement encryption for quantum key distribution. Phys Rev A, 2003, 68: 042315
8 Deng F G, Long G L. Bidirectional quantum key distribution protocol with practical faint laser pulses. Phys Rev A, 2004, 70: 012311
9 Hwang W Y. Quantum key distribution with high loss: Toward global secure communication. Phys Rev Lett, 2003, 91: 057901
10 Lo H K, Chau H F, Ardehali M. Efficient quantum key distribution scheme and a proof of its unconditional security. J Cryptology, 2005, 18: 133–165
11 Wang X B. Quantum key distribution with two-qubit quantum codes. Phys Rev Lett, 2004, 92: 077902
12 Wang X B. Quantum error-rejection code with spontaneous parametric down-conversion. Phys Rev A, 2004, 69: 022320
13 Wang X B. Fault tolerant quantum key distribution protocol with collective random unitary noise. Phys Rev A, 2005, 72: 050304(R)
14 Deng F G, Li X H, Zhou H Y, et al. Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys Rev A, 2005, 72: 044302
15 Li X H, Deng F G, Zhou H Y. Faithful qubit transmission against collective noise without ancillary qubits. Appl Phys Lett, 2007, 91: 144101
16 Li X H, Deng F G, Zhou H Y. Efficient quantum key distribution over a collective noise channel. Phys Rev A, 2008, 78: 022321
17 Xu F X, Chen W, Wang S, et al. Field experiment on a robust hierarchical metropolitan quantum cryptography network. Chinese Sci Bull, 2009, 54: 2991–2997
18 Li C Z. Real applications of quantum communications in China. Chinese Sci Bull, 2009, 54: 2976–2977
19 Zhang X L. One-way quantum identity authentication based on public key. Chinese Sci Bull, 2009, 54: 2018–2021
20 Einstein A, Podolsky B, Rosen N. Can quantum-mechanical description of physical reality be considered complete? Phys Rev, 1935, 47: 777–780
21 Bell J S. On the Einstein-Podolsky-Rosen paradox. Physics, 1965, 1: 195–200
22 Hillery M, Buzek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829–1834
23 Yan F L, Gao T. Quantum secret sharing between multiparty and multiparty without entanglement. Phys Rev A, 2005, 72: 012304
24 Yan F L, Gao T, Li Y C. Quantum secret sharing between multiparty and multiparty with four states. Sci China Ser G-Phys Mech Astron, 2007, 50: 572–580
25 Gao T, Yan F L, Li Y C. Quantum secret sharing between m-party and n-party with six states. Sci China Ser G-Phys Mech Astron, 2009, 52: 1191–1202